IFW

AF $

Attorney Docket No. 1032326-000312

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

Alexandre Benoit et al.

Application No.: 10/553,348

Filed: June 14, 2006

For: METHOD FOR MANAGING AN EXECUTABLE CODE DOWNLOADED IN A REPROGRAMMABLE ON-BOARD SYSTEM

Group Art Unit: 2437

Examiner: Courtney D. Fields

Appeal No.: ______________

APPEAL BRIEF

Mail Stop APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This appeal is from the decision of the Primary Examiner dated April 29, 2009 finally rejecting claims 1-6, which are reproduced as the Claims Appendix of this brief.

☒ Charge □ $ 270 ☒ $ 540 to Credit Card. Form PTO-2038 is attached.

The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.17 and 41.20 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800.

Table of Contents

I. Real Party in Interest

The present application is assigned to GEMPLUS.

II. Related Appeals and Interferences

The Appellant legal representative, or assignee, does not know of any other appeal or interferences which will affect or be directly affected by or have bearing on the Board's decision in the pending appeal.

III. Status of Claims

The application contains claims 1-6. Claims 1-6 are pending, and stand finally rejected. This appeal is directed to all pending claims.

IV. Status of Amendments

There were no Amendments submitted subsequent to the final Office Action.

V. Summary Claimed Subject Matter

The claimed subject matter is directed to a secure procedure for downloading and verifying executable code on a microprocessor card.

The steps of the claimed method can be readily understood with reference to FIGS. 1-3 of the application. The executable code that is intended to be run on the microprocessor card, designated CI', is derived from original executable code CI, and modified for a specific use. Prior to downloading code onto the card, an operation is performed off-card, as depicted in FIG. 1. A software component CL is calculated, based on differences between the original executable code CI and the modified executable code CI'. This software component enables the modified code CI' to be reconstructed from the original code CI. The original executable code CI and the software component CL are signed, to enable their authenticity to be verified.

Thereafter, as depicted in FIG. 2, the signed original code CI and the signed software component CL are loaded onto the card. Then, in an operation which takes place on the card, the signatures of the original code and the software component are verified. Upon verification, the software component CL that was loaded onto the card is applied to the original code CI that was also loaded onto the card, to reconstruct the modified code CI', on the card (FIG. 3). This modified code can then be executed by the card's microprocessor.

Claim 1 is the only independent claim in the present application. A mapping of independent claim 1 to the disclosure is set forth in the following table, which is not to be construed as a representation that the portions of the disclosure identified below constitute the sole basis for support for the claimed subject matter. Please note that the references to the specification are made to the specification submitted in the second Preliminary Amendment dated November 21, 2005.

Claim	Disclosure
1. A method of managing an original executable code forming a program to be downloaded into a reprogrammable on-board computer system in a microprocessor card, said code possessing a cryptographic signature and being executable by the microprocessor of the on-board system after verification by the latter of the validity of said signature, said method comprising the following steps:	
- off card: - identifying a modified executable code corresponding to the original code, adapted to a predefined specific use, and	Page 7, the second paragraph; FIG. 1, CI' and CI
- from variations between the data of the original code and the corresponding modified code, calculating a software component which, when it is applied to the original code, makes it possible to reconstruct the modified code;	Page 7, the second paragraph; page 10, the last full paragraph; FIG. 1, CL, CI' and CI
- signing said software component;	Page 7, the second paragraph; page 10, the last

	full paragraph; FIG. 1, CL'
- downloading the signed original code and the signed software component into the card; and	Page 11, the first full paragraph, FIG. 2, CI, CL and CP
- on card: - verifying the signatures respectively of the original code and of the software component, and	Page 7, the fourth paragraph; page 11, the last full paragraph; FIG. 3, CI, CL
- applying the software component to the original code so as to reconstruct the modified code for its execution by the microprocessor.	Page 7, the fourth paragraph; the paragraph bridging pages 11 and 12, FIG. 3, CI, CL and CI'
[redacted]	[redacted]

VI. Grounds of Rejection to be Reviewed on Appeal

For purposes of this appeal, the Board is being asked to review the following ground of rejection in the final Office Action:

Claims 1-6 stand rejected under 35 U.S.C. §102(e) for allegedly being anticipated by Vetillard (U.S. Patent Publication No. 2005/0107069, hereinafter "Vetillard").

VII. Argument

Claims 1-6 stand rejected under 35 U.S.C. §102 by Vetillard. As set forth in MPEP § 2131, "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." The final Office Action fails to provide a factual showing that meets this requirement. In setting forth the rejection, the Office Action cites to certain passages within the reference. However, the relationship of these passages to the language of the claims is not self-evident. Nor does the Office Action provide any explanation of the manner in which these passages are being interpreted to disclose, either expressly or inherently, the elements recited in the claims. As such, the final Office

Action fails to provide the factual showing that is necessary to support an anticipation rejection of any of the claims.

Claim 1

Claim 1 recites three distinct elements of code, namely (i) original executable code, (ii) modified executable code corresponding to the original code, and (iii) a software component which, when it is applied to the original code, makes it possible to reconstruct the modified code.

Vetillard does not disclose the three distinct elements of code as described in claim 1. Vetillard discloses a method and device for securing messages exchanged over a data transmission network between a server and a client, e.g. a smart card. Referring to FIG. 1 of Vetillard, a representative of the authority 3 is inserted between the server 1 and the client 2.

Referring to FIG. 2 of Vetillard, the representative of the authority 3 sets up two secure channels for exchanging messages: (1) a first secure channel 4, to the server 1, using a first key Ks known to the representative of the authority 3 and to the server 1 but not to the client 2, and using a first encryption algorithm AL, and (2) a second secure channel 5, to the client 2, using a second key Kc known to the representative of the authority 3 and to the client 2 but not to the server 1, and using a second encryption algorithm AL'.

The server 1 sends the code C to be loaded to the representative of the authority 3 via the first secure channel 4. The representative of the authority 3 verifies the properties on the code C. The representative of the authority 3 transmits the verified code to the client via the second secure channel 5.

According to Vetillard, only one element (i.e., the verified code) is loaded in the smart card. However, according to the Appellant's claimed method, two distinct elements, namely the signed original code and the signed software component, are loaded in the smart card. Therefore, Vetillard does not teach or suggest loading two distinct elements of code in the smart card.

The statement of rejection (Office Action at pages 3-4) refers to Vetillard at paragraphs [0058] - [0064] and [0073] - [0074]. These paragraphs describe the loading of code onto the representative of an authority 3, which can be a smart card, and verifying electronic signatures of the code by the representative of an authority 3. Presumably, the Office Action is interpreting this code to be one of the two forms of executable code (either original or modified) that is recited in claim 1. However, the Office Action does not identify any disclosed elements of code that are being interpreted to constitute the other of the two claimed forms of executable code (modified or original).

In addition, Vetillard does not disclose a software component which, when it is applied to the original code, makes it possible to reconstruct the modified code. At best, therefore, the Office Action only contains a showing sufficient to establish that Vetillard discloses one of the elements of code that are recited in the claim, but not all three.

Furthermore, claim 1 recites certain operations that are performed off-card, i.e., before any code is loaded onto the card, and other operations that are performed on-card, after certain elements of code have been loaded. There is no showing that the specific operations respectively performed off-card and on-card with those code elements are carried out in the same manner as recited in the claim.

For example, claim 1 recites that, after identifying modified executable code that corresponds to the original executable code, the following step is performed off-card; "from variations between the data of the original code and the corresponding modified code, calculating a software component which, when it is applied to the original code, makes it possible to reconstruct the modified code". In rejecting claim 1, the Office Action refers to paragraphs [0058] and [0059] of Vetillard in connection with this claimed step. These two paragraphs describe the secure exchange of messages between the server 1 and the client 2, using the representative of a verification authority 3. The Office Action does not explain how they can be interpreted to disclose the calculation of a software component that can be applied to original code to reconstruct the modified code.

Claim 1 recites that, once the signed original code and the signed software component are downloaded to the card and verified, the following operation is performed on-card; "applying the software component to the original code so as to reconstruct the modified code for its execution by the microprocessor." In connection with this claimed feature, the statement of rejection refers to paragraphs

[0073] and [0074] of Vetillard. These paragraphs discuss the verification of electronic signatures by the representative of authority 3. It is not at all apparent, however, how they are being interpreted to disclose the application of a software component to original executable code in order to reconstruct previously identified modified code. Nor does the Office Action provide any explanation of such an interpretation.

In responding to Applicant's prior arguments, paragraph 2 of the Office Action (pages 2-3) discusses paragraphs [0055] - [0057], [0070] and [0073]. In doing so, however, the Office Action does not relate the subject matter disclosed in these paragraphs to the elements of claim 1. Nowhere in this discussion does the Office Action refer to the claim language, or otherwise attempt to identify what subject matter disclosed in these paragraphs, or any other portion of the reference, corresponds to the claimed modified executable code or the claimed software component. Nor does the Office Action address the distinction between the claimed operations that are carried out off-card, and those that are performed on-card.

Accordingly, the Office Action has not established that Vetillard disclose all of the features recited in the rejected claim.

Claim 2

Claim 2 recites a method according to claim 1, wherein the original executable code consists of an intermediate code, executable by the on-board system microprocessor by means of a virtual machine for interpreting this intermediate code.

The Office Action refers to paragraphs 0065-0067 of Vetillard in connection with this claimed feature. Those paragraphs disclose verifying the code by the representative of the authority 3, and transmitting the verified code to the client 2 by the second secure channel 5. Vetillard discloses that the code is executable. See Vetillard: paragraph 0055. However, Vetillard does not disclose that the code is an intermediate code, executable by the on-board system microprocessor by means of a virtual machine for interpreting this intermediate code, as recited in claim 1.

Claim 3

Claim 3 recites a method according to claim 2, wherein the virtual machine is provided with an execution stack and wherein the downloaded software component, which is applied on card to the original intermediate code, makes it possible to reconstruct a modified intermediate code a priori satisfying the verification criteria for said intermediate code according to which the operands of each instruction of said code belong to the data types manipulated by this instruction and, on each target switching instruction, the execution stack of the virtual machine is empty.

The Office Action refers to paragraphs 0056 and 0073 of Vetillard in connection with this claimed feature. Paragraph 0056 of Vetillard discloses that the code must conform to a set of properties that must be verified by a verification authority. Paragraph 0073 of Vetillard discloses that the verification of electronic signatures by the client 2 is problematic if the client is a simple smart card. Even though Vetillard mentions verification of the code, the reference does not disclose any details on verification criteria. In addition, Vetillard does not mention the concept of a virtual machine at all. Therefore, Vetillard could not possibly disclose the method described in claim 3.

Claim 4

Claim 4 is patentable at least because of its dependency from claim 3, and indirectly claim 1.

Claim 5

Claim 5 recites a method according to claim 1, wherein the downloaded software component, applied on card to the original code, makes it possible to reconstruct a modified code so that its execution is more rapid compared with that of the original code.

The Office Action refers to paragraphs 0073 of Vetillard in connection with this claimed feature. Paragraph 0073 of Vetillard discloses that the verification of electronic signatures by the client 2 is problematic if the client is a simple smart card due to the insufficient resources on the smart card. Paragraph 0073 is concerned with the amount of resources available on a smartcard to perform verification of the code. This paragraph is not concerned with speed of execution of code. As explained above, Vetillard does not disclose the concept of original code and the modified code which may be obtained by applying the software component to the original code. Therefore, Vetillard does not disclose that the modified code's execution is more rapid compared with that of the original code, as recited in claim 5.

Claim 6

Claim 6 recites a method according to claim 1, wherein the downloaded software component, applied on card to the original code, makes it possible to reconstruct a modified code so that it procures an optimization in terms of size compared with the original code.

The Office Action refers to paragraphs 0056 and 0073 of Vetillard in connection with this claimed feature. Paragraph 0056 of Vetillard discloses that the code must conform to a set of properties that must be verified by a verification authority. Paragraph 0056 is not concerned with size of code. As mentioned above, paragraph 0073 of Vetillard discloses that the verification of electronic signatures by the client 2 is problematic if the client is a simple smart card due to the insufficient resources on the smart card. As explained above, Vetillard does not disclose the concept of original code and the modified code which may be obtained by applying the software component to the original code. Therefore, Vetillard does not disclose reconstructing a modified code so that in procures an optimization in terms of size compared with that of the original code, as recited in claim 6.

VIII. Claims Appendix

See attached Claims Appendix for a copy of the claims involved in the appeal.

IX. Evidence Appendix

(none)

X. Related Proceedings Appendix

(none)

Respectfully submitted,
BUCHANAN INGERSOLL & ROONEY PC

Date October 21, 2009

By: Weiwei Y. Stiltner
Weiwei Y. Stiltner
Registration No. 62979

Customer No. 21839
703 836 6620

VIII. CLAIMS APPENDIX

The Appealed Claims

1. A method of managing an original executable code forming a program to be downloaded into a reprogrammable on-board computer system in a microprocessor card, said code possessing a cryptographic signature and being executable by the microprocessor of the on-board system after verification by the latter of the validity of said signature, said method comprising the following steps:

- off card:

- identifying a modified executable code corresponding to the original code, adapted to a predefined specific use, and

- from variations between the data of the original code and the corresponding modified code, calculating a software component which, when it is applied to the original code, makes it possible to reconstruct the modified code;

- signing said software component;

- downloading the signed original code and the signed software component into the card; and

- on card:

- verifying the signatures respectively of the original code and of the software component, and

- applying the software component to the original code so as to reconstruct the modified code for its execution by the microprocessor.

2. A method according to claim 1, wherein the original executable code consists of an intermediate code, executable by the on-board system microprocessor by means of a virtual machine for interpreting this intermediate code.

3. A method according to claim 2, wherein the virtual machine is provided with an execution stack and wherein the downloaded software component, which is applied on card to the original intermediate code, makes it possible to reconstruct a modified intermediate code a priori satisfying the verification criteria for said intermediate code according to which the operands of each instruction of said code belong to the data types manipulated by this instruction and, on each target switching instruction, the execution stack of the virtual machine is empty.

4. A method according to claim 3, wherein the modified intermediate code obtained by the application of the software component is verified, before its execution by the microprocessor by means of the virtual machine, according to a process verifying that the modified intermediate code satisfies the verification criteria.

5. A method according to claim 1, wherein the downloaded software component, applied on card to the original code, makes it possible to reconstruct a modified code so that its execution is more rapid compared with that of the original code.

6. A method according to claim 1, wherein the downloaded software component, applied on card to the original code, makes it possible to reconstruct a modified code so that it procures an optimization in terms of size compared with the original code.

IX. EVIDENCE APPENDIX

None

X. RELATED PROCEEDINGS APPENDIX

None